UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/766,060	01/28/2004	Michael A. Aday	MSFT-2858/301129.01	2297

41505 7590 08/13/2007

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
NALVEN, ANDREW L	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
08/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/766,060	ADAY ET AL.	
	Examiner	Art Unit	
	Andrew L. Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) *1-7,20-25 and 32-34* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-19,26-31 and 35-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/28/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-45 are pending. Claims 1-7, 20-25, and 32-34 are withdrawn from consideration.

Election/Restrictions

2. Applicant's election without traverse of Group II which includes claims 8-19, 26-31, and 35-45 in the reply filed on 13 July 2007 is acknowledged.

Claim Rejections - 35 USC § 101

3. **Claims 26-31 are rejected under 35 U.S.C. 101** because the claims are directed towards a computer readable medium that is nonstatutory subject matter. The cited claims are an example of functional descriptive material consisting of data structures and programs that impart functionality only when employed as executed by a computer component. The functionality of functional descriptive material is realized only when the functional descriptive material is claimed as being embodied on a tangible computer readable medium and is claimed as executed by a computer component. The cited claims provide no tangible computer components that work in conjunction with the functional descriptive material to impart functionality and as a result the claims are not

statutory because they fail the practical application requirement of § 101 by failing to provide a useful, concrete, and tangible result (see MPEP 2106).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. **Claims 8-19, 26-31, and 35-45 are rejected under 35 U.S.C. 102(a)** as being anticipated by Anderson et al US Patent No. 6,609,200.

5. **With regards to claim 8**, Anderson teaches a method of protecting a message having information in a multiparty transaction (Anderson, column 18 lines 25-40, protects electronic documents, column 20 lines 54-67, document passes through numerous institutions), the method comprising: obtaining identities of at least two transaction participants in the multiparty transaction (Anderson, column 24 lines 21-35, bank validates payee and payer signatures by identifying them using public key cryptography); obtaining cryptographic information corresponding to the at least two transaction participants (Anderson, column 28 lines 56-67, obtains public keys from directory); dividing the information into segments wherein a relevant portion of the information is placed into at least two segments corresponding to the at least two identities of the transaction participants (Anderson, column 20 lines 54-67, document

divided into new and original information); and cryptographically encoding the divided segments using the cryptographic information corresponding to the transaction participants (Anderson, column 21 lines 1-8, signature added to new information or inner nested information, column 20 lines 14-48, original electronic document is bound together by a signature block).

6. **With regards to claim 9,** Anderson teaches obtaining identities of at least two transaction participants comprises acquiring the identities from one of the transaction participants (Anderson, column 28 lines 56-67, payee can furnish his public key, column 28 lines 10-20, payer sends public key).

7. **With regards to claim 10,** Anderson teaches obtaining cryptographic information comprises acquiring cryptographic information from at least one of a directory and cryptographic identity provider (Anderson, column 28 lines 56-67, obtains public keys from directory).

8. **With regards to claim 11**, Anderson teaches the cryptographic identity provider is not one of the transaction participants (Anderson, column 28 lines 56-67, obtains public keys from public directory).

9. **With regards to claim 12,** Anderson teaches dividing the information into segments comprises placing only a portion of the information which is needed by a particular transaction participant into a segment encrypted for the particular participant (Anderson, column 20 lines 31-47, hash of content is encrypted to form signature which is needed by other party to verify authenticity).

10. **With regards to claim 13,** Anderson teaches transmitting a cryptographically encoded segment to only a cryptographically corresponding transaction participant (Anderson, column 23 lines 30-41, cryptographically sealed passing across network).

11. **With regards to claim 14,** Anderson teaches transmitting the cryptographically encoded segments to the at least two transaction participants (Anderson, column 23 lines 30-41, cryptographically sealed passing across network).

12. **With regards to claim 15**, Anderson teaches a method of controlling data content exposure in a multiparty transaction (Anderson, column 18 lines 25-40, protects electronic documents, column 20 lines 54-67, document passes through numerous institutions), the method comprising: obtaining, from a primary transaction participant, at least two identities of secondary transaction participants to be involved in a multiparty transaction (Anderson, column 24 lines 21-35, bank validates payee and payer signatures by identifying them using public key cryptography); obtaining cryptographic information for the at least two secondary transaction participants (Anderson, column 28 lines 56-67, obtains public keys from directory), each secondary transaction participant having unique cryptographic information (Anderson, column 24 lines 21-47, payee and payer having public keys and private keys); cryptographically encoding information for the at least two secondary transaction participants such that a data content and unique encryption are used for each secondary transaction participant (Anderson, column 21 lines 1-8, signature added to new information or inner nested information, column 20 lines 14-48, original electronic document is bound together by a signature block); and

transmitting the cryptographically encoded information (Anderson, column 23 lines 30-41, cryptographically sealed passing across network).

13. **With regards to claim 16**, Anderson teaches transmitting the cryptographically encoded information comprises transmitting the cryptographically encoded information to the primary transaction participant (Anderson, column 23 lines 30-41, cryptographically sealed passing across network, column 24 lines 20-25, bank receives endorsed instrument).

14. **With regards to claim 17,** Anderson teaches receiving status from the primary transaction participant concerning a successful examination of data content by one or more of the at least two secondary transaction participants, whereby multiparty transaction status is assessed (Anderson, column 23 line 42 – column 24 line 20, payee verifies payer signature and payer verifies payee signature before providing document to bank).

15. **With regards to claim 18**, Anderson teaches cryptographically encoding information for the at least two secondary transaction participants comprises encoding a data content that is unique for at least one of the at least two secondary transaction participants (Anderson, column 23 lines 40-67, payee content is a memorandum of a proposed transaction while payer content is a financial instrument).

16. **With regards to claim 19,** Anderson teaches transmitting a message request to act upon the information represented by the data content so as to execute the multiparty transaction (Anderson, column 24 lines 10-25, sends request to bank to execute the transaction).

17. **With regards to claim 26**, Anderson teaches a computer-readable medium having computer-executable instructions for performing a method of protecting a message having information in a multiparty transaction (Anderson, column 18 lines 25-40, protects electronic documents, column 20 lines 54-67, document passes through numerous institutions, column 18 lines 40-60, client computers), the method comprising: obtaining identities of at least two transaction participants in the multiparty transaction (Anderson, column 24 lines 21-35, bank validates payee and payer signatures by identifying them using public key cryptography); obtaining cryptographic information corresponding to the at least two transaction participants (Anderson, column 28 lines 56-67, obtains public keys from directory); dividing the information into segments wherein a relevant portion of the information is placed into at least two segments corresponding to the at least two identities of the transaction participants (Anderson, column 20 lines 54-67, document divided into new and original information); and cryptographically encoding the divided segments using the cryptographic information corresponding to the transaction participants (Anderson, column 21 lines 1-8, signature added to new information or inner nested information, column 20 lines 14-48, original electronic document is bound together by a signature block).

18. **With regards to claim 27**, Anderson teaches obtaining identities of at least two transaction participants comprises acquiring the identities from one of the transaction participants (Anderson, column 28 lines 56-67, payee can furnish his public key, column 28 lines 10-20, payer sends public key).

19. **With regards to claim 28**, Anderson teaches obtaining cryptographic information comprises acquiring cryptographic information from at least one of a directory and cryptographic identity provider (Anderson, column 28 lines 56-67, obtains public keys from directory).

20. **With regards to claim 29,** Anderson teaches dividing the information into segments comprises placing only a portion of the information which is needed by a particular transaction participant into a segment encrypted for the particular participant (Anderson, column 20 lines 31-47, hash of content is encrypted to form signature which is needed by other party to verify authenticity).

21. **With regards to claim 30,** Anderson teaches transmitting a cryptographically encoded segment to only a cryptographically corresponding transaction participant (Anderson, column 23 lines 30-41, cryptographically sealed passing across network).

22. **With regards to claim 31,** Anderson teaches transmitting the cryptographically encoded segments to the at least two transaction participants (Anderson, column 23 lines 30-41, cryptographically sealed passing across network, column 23 line 42 – column 24 line 20, payee verifies payer signature and payer verifies payee signature before providing document to bank).

23. **With regards to claim 35,** Anderson teaches a system comprising: a processor having access to memory, the memory having instructions which, when executed, perform the method of protecting a message having information in a multiparty transaction (Anderson, column 18 lines 25-40, protects electronic documents, column 20 lines 54-67, document passes through numerous institutions, column 18 lines 40-60,

client computers), the method comprising: obtaining identities of at least two transaction participants in the multiparty transaction (Anderson, column 24 lines 21-35, bank validates payee and payer signatures by identifying them using public key cryptography); obtaining cryptographic information corresponding to the at least two transaction participants (Anderson, column 28 lines 56-67, obtains public keys from directory); dividing the information into segments wherein a relevant portion of the information is placed into at least two segments corresponding to the at least two identities of the transaction participants (Anderson, column 20 lines 54-67, document divided into new and original information); and cryptographically encoding the divided segments using the cryptographic information corresponding to the transaction participants (Anderson, column 21 lines 1-8, signature added to new information or inner nested information, column 20 lines 14-48, original electronic document is bound together by a signature block).

24. **With regards to claim 36,** Anderson teaches the instructions having the method step of obtaining identities of at least two transaction participants comprise acquiring the identities from one of the transaction participants (Anderson, column 28 lines 56-67, payee can furnish his public key, column 28 lines 10-20, payer sends public key).

25. **With regards to claim 37,** Anderson teaches the instruction having the method step of obtaining cryptographic information comprise acquiring cryptographic information from at least one of a directory and cryptographic identity provider (Anderson, column 28 lines 56-67, obtains public keys from directory).

26. **With regards to claim 38,** Anderson teaches the instructions having the method step of dividing the information into segments comprise placing only a portion of the information which is needed by a particular transaction participant into a segment encrypted for the particular participant (Anderson, column 20 lines 31-47, hash of content is encrypted to form signature which is needed by other party to verify authenticity).

27. **With regards to claim 39,** Anderson teaches transmitting a cryptographically encoded segment to only a cryptographically corresponding transaction participant (Anderson, column 23 lines 30-41, cryptographically sealed passing across network).

28. **With regards to claim 40,** Anderson teaches the instructions performing the method further comprise: transmitting the cryptographically encoded segments to the at least two transaction participants (Anderson, column 23 lines 30-41, cryptographically sealed passing across network, column 23 line 42 – column 24 line 20, payee verifies payer signature and payer verifies payee signature before providing document to bank).

29. **With regards to claim 41,** Anderson teaches a processor having access to memory, the memory having instructions which, when executed, perform the method of controlling data content exposure in a multiparty transaction (Anderson, column 18 lines 25-40, protects electronic documents, column 20 lines 54-67, document passes through numerous institutions, column 18 lines 40-60, client computers), the method comprising: obtaining, from a primary transaction participant, at least two identities of secondary transaction participants to be involved in a multiparty transaction (Anderson, column 24 lines 21-35, bank validates payee and payer signatures by identifying them using public

key cryptography); obtaining cryptographic information for the at least two secondary transaction participants (Anderson, column 28 lines 56-67, obtains public keys from directory), each secondary transaction participant having unique cryptographic information; cryptographically encoding information for the at least two secondary transaction participants such that a data content and unique encryption are used for each secondary transaction participant; and transmitting the cryptographically encoded information (Anderson, column 21 lines 1-8, signature added to new information or inner nested information, column 20 lines 14-48, original electronic document is bound together by a signature block).

30. **With regards to claim 42,** Anderson teaches the instructions performing the method step of transmitting the cryptographically encoded information comprise transmitting the cryptographically encoded information to the primary transaction participant (Anderson, column 23 lines 30-41, cryptographically sealed passing across network, column 23 line 42 – column 24 line 20, payee verifies payer signature and payer verifies payee signature before providing document to bank).

31. **With regards to claim 43,** Anderson teaches the instructions performing the method further comprise: receiving status from the primary transaction participant concerning a successful examination of data content by one or more of the at least two secondary transaction participants, whereby multiparty transaction status is assessed.

32. **With regards to claim 44,** Anderson teaches the instructions performing the method step of cryptographically encoding information for the at least two secondary transaction participants comprise encoding a data content that is unique for at least one

of the at least two secondary transaction participants (Anderson, column 23 lines 40-67, payee content is a memorandum of a proposed transaction while payer content is a financial instrument).

33. **With regards to claim 45,** Anderson teaches the instructions performing the method steps further comprise transmitting a message request to act upon the information represented by the data content so as to execute the multiparty transaction (Anderson, column 24 lines 10-25, sends request to bank to execute the transaction).

Conclusion

34. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

35. Fox et al US Patent No. 7,003,480 discloses a system for standards based electronic commerce transactions.

36. Walker et al US Patent No. 6,904,418 discloses a method for executing cryptographically enabled letters of credit.

37. Leong et al US Patent No. 7,167,844 discloses an electronic menu document creator in a virtual financial environment.

38. Hawkins et al US Patent No. 7,146,500 discloses a system for obtaining signatures on a single authoritative copy of an electronic record.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Andrew Nalven